

## Bilag 1. Handleplaner til revisionsbemærkninger den løbende revision 2024

Nedenfor ses samtlige bemærkninger på de tre områder, som revisionen har afgivet i forbindelse med den løbende revision. De grønt markerede bemærkninger er dem, som SUF har skulle forholde sig til. På baggrund af bemærkningerne har SUF udarbejdet handleplaner, og disse fremgår efter oversigten.

### Oversigt over afgivne bemærkninger fra revisionen:

<b>Bemærkninger i den løbende revision vedr. Regnskabsføring, forretningsgange og interne kontroller 2024</b>	
3.1.1.1 Administration af autorisationer til Kvantum (rød)	Økonomiforvaltningen
3.1.1.2 Administration af autorisationer til Kvantum (gul)	Økonomiforvaltningen
3.1.2.1 Bilagskontrol (gul)	Børne- og Ungdomsforvaltningen, Socialforvaltningen
3.1.2.2 Bilagskontrol (grøn)	Sundheds- og Omsorgsforvaltningen, Teknik- og Miljøforvaltningen, Økonomiforvaltningen
3.2.1.1 Brugeradministration Kvantum (SAP Basis) (rød)	Økonomiforvaltningen
3.2.1.2 Brugeradministration (privilegerede brugere) (gul)	Økonomiforvaltningen
3.2.2.1 Kreditor (grøn)	Forvaltningerne
<b>Bemærkninger i den løbende revision vedr. Generelle IT-kontroller 2024</b>	
3.1.1 Organisering af informationssikkerhed og styrkelse af ISMS (rød)	Økonomiforvaltningen
3.1.2 Risikovurderinger af it-systemer (rød)	Økonomiforvaltningen
3.1.3 Åbning af det produktive miljø (Kvantum) (rød)	Økonomiforvaltningen
3.1.4 Log af åbninger (Kvantum) (rød)	Økonomiforvaltningen
3.1.5 Password opsætning (Kvantum) (gul)	Økonomiforvaltningen
3.1.6 Gennemgang af rettigheder (Kvantum) (gul)	Økonomiforvaltningen
3.2.1 Ledelsestilsyn med bruger autorisationer (rød)	Forvaltningerne
3.2.2 Sikkerhedsvurdering af systemer	Forvaltningerne
<b>Bemærkninger i den løbende revision vedr. Revision af løn- og personaleområdet 2024</b>	
4.4 Afregning til Feriefonden (rød)	Forvaltningerne
4.1 Arbejdsskade (gul)	Økonomiforvaltningen
4.3 Sagsgennemgang (grøn)	Økonomiforvaltningen
4.2 VIP-kontrol (grøn)	Økonomiforvaltningen

### Forslag til handleplan vedr. ledelsestilsyn med brugerautorisationer

<b>3.2.1 Ledelsestilsyn med brugerautorisationer</b>	
Farvemarkering (prioritet)	Rød
Gives til	Forvaltningerne
<b>Observationer og risici:</b>	
<i>Ledelsestilsyn med brugerautorisationer</i>	
Det er i KK besluttet, at IT-systemer med adgangsstyring, som håndterer per-son- eller værdioplysninger, skal integreres med kommunens til enhver tid anvendte brugerstyringsløsning til bestilling af autorisationer.	

Hvis integration til den gældende brugerstyringsløsning fravælges, skal fravalget dokumenteres og forelægges for ØKF, som efter koordinering med IT-kredsen kan meddele dispensation herfra. Det sker ikke konsekvent i dag.

Kommunen skal føre en ajourført fortegnelse over alle væsentlige informationsaktiver.

I KK er fortegnelsen i FISKK og indeholder ca. 1.400 informationsaktiver/systemer, som kan være infrastrukturelementer, systemer m.v.

Det skal aktivt sikres, at informationer er korrekt mærkede i forhold til det fastlagte dataklassifikationssystem med henblik på at leve op til gældende regler.

Forvaltningerne oplyser, at der er stor usikkerhed omkring de registrerede oplysninger i FISKK, som systemejerne har til opgave at ajourføre.

Systemer integreret i kommunens IGA-løsning inddeles efter kritikalitet, hvor der for systemer med person- og værdioplysninger skal udføres manuelt tilsyn med, om tildelte autorisationer afspejler medarbejdernes arbejdsmæssige behov, minimum hvert år eller hvert andet år. Forvaltningerne har oplyst, at ledelsestilsyn ikke fuldt ud er udført i overensstemmelse med reglerne, og at udeståender er planlagt gennemført hurtigst muligt.

For en stor del af systemerne med brugere eller som håndterer person- eller værdioplysninger, er den valgte brugerstyringsløsning fravalgt eller ikke teknisk mulig.

Det betyder som udgangspunkt, at der hver 6. måned manuelt skal foretages tilsyn med, om tildelte autorisationer afspejler medarbejdernes arbejdsmæssige behov. Ifølge forvaltningernes oplysninger foretages de halvårslige tilsyn med tildelte autorisationer kun i mindre grad.

Endelig ses der ikke at være taget stilling til, hvordan de væsentlige strategiske mål og forretningsmæssige gevinster, der sikres i IGA-løsningen, sikres for systemer uden for IGA-løsningen.

#### **Status 2024**

Forvaltningernes har besluttet og igangsat en handleplan som omfatter:

1. Udførelse af ledelsestilsyn, jf. KK's regler
2. Korrekt mærkning i forhold til det fastlagte dataklassifikationssystem i kommunens fortegnelse FISKK
3. Onboarding af systemer i brugerstyringsløsningen
4. Genbesøg af informationssikkerhedscirkulæret
5. Fortsættelse af igangværende udviklingsopgaver mhp. Effektiv administration.

Handleplanen forventes gennemført i perioden Q4 2024 til ultimo 2025.

<b>Revisionsbemærkning:</b>	<b>Berørt(e) forvaltning(er):</b>
Bemærkningen videreføres og i lighed med tidligere år henstilles til, at: <ul style="list-style-type: none"><li>➤ de ledelsestilsyn, som skal sikre, at de ansatte ikke har adgang til personoplysninger, hvor der ikke er et arbejdsbetinget behov, udføres i overensstemmelse med kommunens regler. Det gælder både de systemer, der er integreret i IGA-løsningen, og de systemer, der ligger uden for IGA-løsningen</li><li>➤ det aktivt sikres, at systemer er korrekt mærkede i forhold til det fastlagte dataklassifikationssystem i kommunens fortegnelse FISKK</li></ul>	Forvaltningerne

<ul style="list-style-type: none"> <li>➤ alle kommunens systemer med adgangsstyring og værdi- og personoplysninger, hvis det er teknisk muligt, integreres i kommunens IGA-løsning</li> <li>➤ der tages stilling til, hvordan de væsentlige strategiske mål og forretningsmæssige gevinster, der sikres i IGA-løsningen, sikres for de 587 systemer, som på nuværende tidspunkt ikke er i IGA-løsningen, og de 39 systemer, hvor det ikke teknisk er muligt at blive tilmeldt IGA-løsningen, bør være særligt kritiske.</li> </ul> <p>Det anbefales herudover, at:</p> <ul style="list-style-type: none"> <li>➤ ledelsestilsynene for systemer integreret i kommunens IGA-løsning opstartes automatisk</li> <li>➤ Kommunens regler (governance) revurderes og beskrives i en fælles administrativ forretningsgang, hvor der fokuseres på at skabe gennemsigtighed i hvordan og hvilke strategiske mål og forretningsmæssige gevinster, der operationaliseres/sikres for fuldt ud at realisere målet om at reducere ressourceforbruget på området væsentligt og forbedre brugeroplevelsen for autorisationsansvarlige og ledere.</li> </ul>	
Handleplan	Status januar 2025
<p><b>Sundheds- og Omsorgsforvaltningen</b></p> <p>SUF indgår i initiativerne i den tværgående handleplan og viderefører dertil i egen forvaltning indsatserne opstartet i 2023 med fokus på kravene til ledelsestilsyn med autorisationer.</p> <p>I forlængelse af ovenstående indeholder SUF's handleplan følgende tiltag.</p> <p><i>Pkt. 1</i> Gennemgang af it-systemporteføljen i forvaltningen med sikring af, at gennemførelse af tilsyn sker i overensstemmelse med kommunens regler.</p> <p><i>Pkt. 2</i> Gennemgang af, om der er yderligere systemer i forvaltningen, der kan være relevante at onboard på IGA og migrering af disse.</p> <p><i>Deadline: Q2 2025</i></p>	<p><b>Sundheds- og Omsorgsforvaltningen</b></p> <p>Pkt. 1: I proces Alle systemer, der styres gennem KK's fælles brugerstyringsløsning vil fremadrettet få gennemført ledelsestilsyn af Brugerstyring i Koncern IT (jf. den fælles handleplan på området). Systemer udenfor den fælles løsning (manuelt brugerstyrede) får fremadrettet gennemført ledelsestilsyn hvert halve år, som led i Systemteamets årshjul. Opgaven er forankret i Systemteamet i Center for Digitalisering.</p> <p>Pkt. 2: I proces Der er udarbejdet et overblik over systemer, der kan onboardes den fællesbrugerstyringsløsning. 7 systemer skal onboardes hvis det er teknisk muligt. Arbejdet med at onboard systemer fortsætter ind i 2025.</p>

## Forslag til handleplan vedr. sikkerhedsvurdering af systemer

3.2.2 Sikkerhedsvurdering af systemer	
Farvemarkering (prioritet)	Rød
Gives til	Forvaltningerne
<p><b>Observationer og risici:</b></p> <p><i>Sikkerhedsvurdering af systemer</i></p> <p>Af Forretningscirkulæret for IT-anskaffelser, der er bindende for alle forvaltninger, fremgår det, at et nyt IT-system skal sikkerhedsvurderes, inden det idriftsættes.</p> <p>En sikkerhedsvurdering tager stilling til, at alle krav til informationssikkerhed og databeskyttelse er opfyldt. På baggrund af sikkerhedsvurderingen udstedes en ibrugtagningstilladelse. IT-systemer skal have en ibrugtagningstilladelse, inden de idriftsættes.</p> <p>Det er forbundet med stor risiko for kommunen at idriftsætte et IT-system uden en sikkerhedsvurdering og en ibrugtagningstilladelse.</p> <p>I 2023 konstaterede vi, at der, jf. oplysningerne i FISKK, er mange systemer, som er anskaffet før 1. november 2018, der ikke har en ibrugtagningsstatus, og at flere systemer har en "ikke-godkendt" status. Altså skulle systemerne ikke være i drift, fordi sikkerheden ikke har levet op til kommunens krav.</p> <p><b>Status 2024</b></p> <p>Forvaltningernes har besluttet og igangsat en handleplan, som omfatter:</p> <ol style="list-style-type: none"> <li>KIT foretager en tilpasset sikkerhedsvurdering af             <ol style="list-style-type: none"> <li>IT-systemer i drift fra før 2018, der har undergået væsentlige ændringer,</li> <li>IT-systemer ibrugtaget før 2018 uden ibrugtagningstilladelse, men hvor der efterfølgende er foretaget en risikovurdering,</li> </ol> </li> <li>KIT gennemgår systemer registreret som "ikke-godkendt" i FISKK og går i dialog med relevante forvaltninger om nødvendigheden af eskalation, ny sikkerhedsvurdering eller udfasning af ikke-godkendte IT-systemer.</li> </ol> <p>Handleplanen forventes gennemført i perioden Q4 2024 til Q2 2025.</p>	
<b>Revisionsbemærkning:</b>	<b>Berørt(e) forvaltning(er):</b>
<p>Bemærkningen videreføres og i lighed med tidligere år henstilles det, at</p> <ul style="list-style-type: none"> <li>➤ de systemer, der ikke har en ibrugtagningsstatus, bliver gennemgået og oplysningerne i FISKK bliver opdateret.</li> <li>➤ der udføres en tilpasset sikkerhedsvurdering af systemer ibrugtaget før 2018.</li> <li>➤ de systemer, der har status "ikke-godkendt" eskaleres, jf. anskaffelsescirkulæret, og der træffes de nødvendige foranstaltninger, blandt andet om udfasning, idet disse, jf. kommunes regler, udgør en sikkerhedsrisiko.</li> </ul>	Forvaltningerne
<b>Handleplan</b>	<b>Status januar 2025</b>
<p><b>Sundheds- og Omsorgsforvaltningen</b></p> <p>SUF følger aktiviteterne i den tværgående handleplan udarbejdet af Koncern IT på baggrund af ovenstående revisionsbemærkninger.</p>	<p><b>Sundheds- og Omsorgsforvaltningen</b></p> <p>Pkt. 1 Gennemført</p>

<p>I forlængelse af disse aktiviteter er der i SUF udarbejdet følgende handleplan:</p> <p><i>Pkt. 1</i> For de it-systemer uden ibrugtagingsstatus, der har systemejerskab i SUF, sikrer SUF opdatering af it-systemoplysninger i KK's it-systemregister (FISKK) inden for deadline fastsat af Koncern IT.</p> <p><i>Pkt. 2</i> De systemansvarlige i SUF udfører kritikalitets-scoring af systemer udvalgt af Koncern IT på baggrund af opdaterede systemoplysninger, jf. punkt 1. Efter afsluttet kritikalitetsscoring igangsættes en sikkerhedsvurdering hos KIT Sikkerhed. <i>Deadline er 31. juli.</i></p> <p><i>Pkt. 3</i> SUF igangsætter i samarbejde med Koncern IT enten godkendelse eller udfasning af systemer med status 'ikke godkendt'. <i>Deadline Q4 2024</i></p> <p><b><u>Deadline for samlet handleplan:</u></b> Indsætterne i handleplanen for håndtering af revisionsbemærkningen forventes afsluttet Q2 2025.</p>	<p>Pkt. 2 Gennemført</p> <p>Pkt. 3 2 systemer med status 'ikke godkendt' er klar-meldt til sikkerhedsvurdering hos Koncern IT (KIT). KIT's vurdering afventes med forventning om at der gives de relevante ibrugtagningstilladelser inden deadline i den fælles handlingsplan, Q2 2025.</p>
---	---

#### Forslag til handleplan vedr. afregning til Feriefonden

<b>4.4 Afregning til Feriefonden</b>	
Farvemærkning (prioritet)	Rød
Gives til	Forvaltningerne
<p><b>Observationer og risici:</b> Vi har konstateret, at der er fejl i grundlaget for de 6 mio. kr. som KK har afregnet til Feriefonden i 2023 for optjeningsåret 2021/2022.</p> <p>Helt overordnet er det vores opfattelse, at medarbejderne enten skal afholde deres ferie eller ferien skal overføres grundet feriehindring m.v. Således bør afregningen på medarbejderniveau typisk være på et uvæsentligt niveau.</p> <p>Vi har i samarbejde med KS foretaget en gennemgang af de 10 højeste afregninger. Gennemgangen viser fejlagtige afregninger, der kan henføres til KS og overvejende sandsynlig, fejlagtig administration i forvaltningerne.</p> <p>Væsentlige afregninger på medarbejderniveau kan typisk henføres til ikke-indberettet ferie, hvilket medfører en dobbeltudgift for KK eller fejl i håndteringen af ferie i forbindelse med fratrædelser, feriehindring m.v., som medfører mistet ferie for medarbejderne.</p>	

Der er medio november 2024 afregnet 4,5 mio. kr. til Feriefonden vedr. optjeningsåret 2022/2023. På baggrund af vores observationer, jf. ovenfor, har KS nået at berigtige 0,5 mio. kr. De konstaterede fejl understøtter vores vurdering af, at der er væsentlige fejl i håndteringen af medarbejdernes ferie, der medfører fejlagtig afregning til Feriefonden.

<b>Revisionsbemærkning:</b>	<b>Berørt(e) forvaltning(er):</b>
<p>KS har tilrettelagt og implementeret flere fornuftige tiltag, der skal medvirke til at sikre en korrekt håndtering af ferie i forvaltningerne.</p> <p>Det er vores vurdering, at de tilrettelagte processer ikke er tilstrækkeligt effektive i forhold til at sikre mod fejl i håndteringen af medarbejdernes ferie. For at sikre, at medarbejderne får overført den ferie de er berettiget til, og at KK ikke får et økonomisk tab, henstiller vi til, at KS i samarbejde med forvaltningerne tilrettelægger en mere effektiv proces.</p> <p>Desuden henstiller vi til, at KS så vidt muligt berigtiger de konstaterede fejl, der kan henføres til KS.</p>	<p>Forvaltningerne</p>
<b>Handleplan januar 2025</b>	<b>Opfølgingsplan</b>
<p><b>Sundheds- og Omsorgsforvaltningen</b></p> <p>KS har igangsat en handlingsplan på vegne af alle forvaltninger. Der er herudover planlagt en temadrøftelse i HR-kredsen ultimo januar 2025, mhp. at drøfte initiativer til korrekt registrering af ferie med henblik på at KS udarbejder en fælles tværgående løsning.</p> <p>Sundheds- og Omsorgsforvaltningen følger den fælles KK-handleplan og iværksætter i forlængelse af denne følgende forvaltningsspecifikke initiativer:</p> <ul style="list-style-type: none"> <li>• Orientering af alle ledere via ugepakken tre gange årligt forud for kontrol med ferie. Den lokale leder har ansvar for at sikre, at kontrollen følges.</li> <li>• Central opfølgning på ferienesaldi ifm. at KS sender advis til lederne om uafholdt ferie. Det samlede overblik deles med lederne i SUF</li> <li>• Ved behov bistår HR med hjælp til proces for opfølgning på den enkelte enhed</li> </ul> <p>Indsatserne har til formål at skærpe opmærksomheden blandt lederne i SUF ift., at ferie afholdes og registreres korrekt.</p> <p>I forbindelse med møde i HR-kredsen i januar vurderes det, om der er behov for yderligere indsatser.</p>	<p><b>Sundheds- og Omsorgsforvaltningen</b></p> <p>I opfølgningen på den fælles handleplan kontrolleres følgende:</p> <ul style="list-style-type: none"> <li>• Kontrol af om initiativer vedr. feriehindring er iværksat</li> <li>• Kontrol af om arbejdsgange er opdaterede for fratrædelse og håndtering af restferie</li> <li>• Kontrol af processen for godkendelse af medarbejders ferie er opdateret og bliver fulgt.</li> </ul> <p>Deadline for opfølgning på handlingsplanen er ultimo juni 2025.</p> <p>I opfølgningen på de forvaltningsspecifikke indsatser kontrolleres følgende: at den centrale opfølgning viser faldende udestående i SUF til Feriefonden</p>